In the claims:

1. (Currently amended) A method for providing ~~highly~~ secure access of a partner to the development environment of another partner comprising the steps of:

starting a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified with a different VPN group/password;

starting a session by the partner in a Web page on a portal machine that authenticates through LDAP (Lightweight Directory Access Protocol) the ~~user/password~~ user identification and password of ~~the~~ a ~~person~~ user;

routing the session to an engagement box of a plurality of engagement boxes depending on the ~~person~~ user where the engagement box~~es~~ includes a server with an operating system and each of said engagement boxes are on network segments separated by firewall boxes with another logon/password and is validated thru second LDAP and wherein all users of the same partner are all launching on the same engagement box ; ~~and~~

accessing data and applications from that engagement box on Network File system storage authenticated second LDAP to get benefit of a big compute server farm composed of many high-end servers in a ~~very~~ secure way; submitting batch or interactive jobs to said server farm on a common resource segment so data input and data output on the server farm remains on the common resource segment; and a display is sent back to appropriate partner's engagement box and then a remote display at the partner location. .

2. (Currently amended) The method of Claim 1 including the step of ~~submitting batch or interactive jobs to a server farm on a common resource segment so data~~

~~input and data output on the server farm remains on a common resource the~~ only a remote display is going back to ~~the engagement box~~ a client device of the partner.

3. (Currently amended) A method of enabling a collaborative network with partners without compromising Intellectual Property comprising the steps of:

providing a ~~highly~~ secure common resource computing zone with services such as design and production wherein data input and output remains on the secure common resource computing zone; ~~and~~

providing multiple layers of security to separate isolated engagement boxes for each of the partners in said secure common resource computing zone where the engagement boxes each include a server with an operating system and where partners can work simultaneously, run simulation tests, emulate software problems and share in said secure common resource computing zone with just ~~the~~ a remote display going back to the engagement box of the partner and therefore to the partner outside the owner; and

submitting batch or interactive jobs to a server on said common resource computing zone so data input and data output on the server on said common resource remains on said common resource computing zone but just a remote display is going back to the engagement box of the partner and then remote display at the partner location.

4. (Original) The method of Claim 3 including the step of said partners running local applications on said engagement boxes such as design applications, mail, editor, etc. or on a server farm segment that resides on the secure common resource computing zone for bigger batch or interactive jobs.

5. (Original) The method of Claim 3 including the step of providing a backend segment that includes an intranet access through a firewall to an owner's intranet.

6. (Original) The method of Claim 5 including the step of providing an access box for management of all critical boxes in said secure computing zone.

7. (Currently amended) The method of Claim 3 wherein said providing layers of security step includes the steps of:

starting a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified with a different VPN group/password;

starting a session by the partner in a Web page on a portal machine that authenticates through LDAP ~~the user/password~~ user identification and password of a user ~~the person~~;

routing the session to an engagement box depending on the ~~person~~ user where the engagement boxes are on network segments separated by firewall boxes with another logon/password and is validated thru second LDAP and wherein all users of the same partner are all launching on the same engagement box; said engagement box including a server with an operating system; and

accessing data and applications from that engagement box on Network File system storage authenticated second LDAP to get benefit of a big compute farm composed of many high-end servers in a ~~very~~ secure way.

8. (Currently amended) A system for providing highly secure access of a partner to the development environment of another partner comprising:

means for providing a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified with a different VPN group/password;

means for starting a session by the partner in a Web page on a portal machine that authenticates thru LDAP ~~the user/password~~ user identification and password of ~~the person~~ a user ;

means for routing the session to an engagement box depending on the person where ~~the~~ engagement boxes are on network segments separated by firewall boxes with another logon/password and is validated thru second LDAP and wherein all users of the same partner are all launching on the same engagement box; said engagement box including a server with an operating system; and

means for accessing data and applications from that engagement box on Network File system storage authenticated second LDAP to get benefit of a big compute farm composed of many high-end servers in a ~~very~~ secure way.

9. (Currently amended) The system of Claim 8 including means for submitting batch or interactive jobs to a server farm on a common resource segment so data input and data output on the server farm remains on ~~a~~ the common resource segment but ~~the~~ a remote display is going back to the engagement box and then remote display at the partner location.

10. (Currently amended) A system for enabling collaboration by an owner of a collaborative network with partners such as sub-contractors, customers and/or Electronic Design Automation (EDA) vendors without compromising Intellectual Property comprising:

a ~~highly~~ secure common resource computing zone with services wherein data input and output remains on the secure common resource computing zone; ~~and~~

means for providing multiple levels of security to separate isolated engagement boxes for each partner in said secure common resource computing zone where said engagement boxes each include servers with an operating system where the partners can work simultaneously, run simulation tests, emulate software problems or share in said secure common resource computing zone with just ~~the~~ a remote display ~~is~~ going back to the engagement box of the partner and therefore to the partner outside the owner and means for submitting batch or interactive jobs to a server on said common resource computing zone so data input and data output on the server on said common resource remains on said common resource computing zone but just a remote display is going back to a client device of the partner.

11. (Original) The system of Claim 10 wherein said partners can run local applications on said engagement boxes such as design applications, mail, editor, etc or on a server farm segment that resides on the common resources zone for bigger batch or interactive jobs.

12. (Original) The system of Claim 10 including a backend segment that includes an owner's intranet access through a firewall to an owner's intranet.

13. (Original) The system of Claim 12 including an access box for management of all critical boxes in said secure computing zone.

14. (Currently amended) The system of Claim 10 wherein said means for providing security includes means for providing a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified

with a different VPN group/password; means for starting a session by the partner in a Web page on a portal machine that authenticates thru LDAP ~~the user/password~~ user identification and password of ~~the person~~ a user; means for routing the session to an engagement box depending on the person where the engagement boxes are on network segments separated by firewall boxes with another logon/password and is validated thru second LDAP and wherein all users of the same partner are all launching on the same engagement box; said engagement box including a server with an operating system and means for accessing data and applications from that engagement box on Network File system storage authenticated second LDAP to get benefit of a big compute farm composed of many high-end servers in a ~~very~~ secure way.